→ What is Cyber Security ?

The technique of protecting internet-connected systems such as computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks is known as cybersecurity.

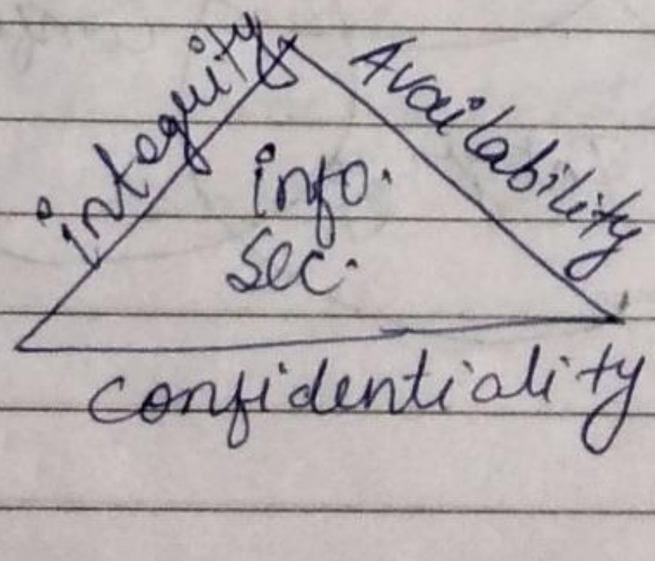
→ Types of Cyber Security:

We can categorize cybersecurity in the following sub-domain:-

- Network security
- Application "
- Info. or data "
- Identity management
- Operational security.

Cyber Security Goals

Cyber Security's main objective is to ensure data protection.
The security community provides a triangle of three related principles to protect data from cyber-attacks. This principle is called the CIA triad.



Date :
Page :

Confidentiality

It is equivalent to privacy that avoids unauthorized access of information. It involves ensuring the data is accessible by those who are allowed to use it and blocking access to others.

It prevents essential information from reaching the wrong people.

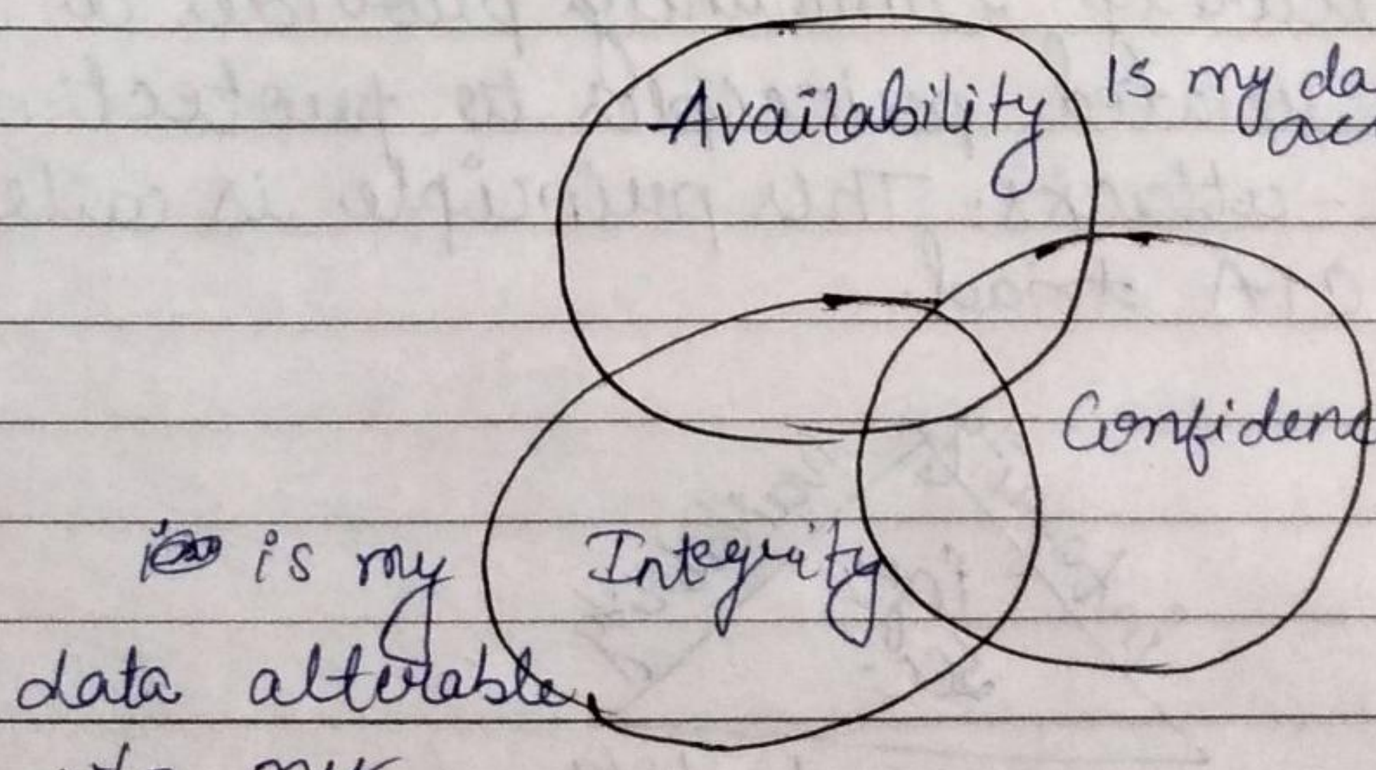
Data encryption is an excellent example of ensuring confidentiality.

Integrity —

↳ data has not been altered in an unauthorized manner.

Availability :

↳ Information can be accessed and modified by authorized individuals in an appropriate timeframe.



Tools for confidentiality	Tools for Integrity:
- Encryption - Access Control - Authentication - Authorization - Physical security	- Backups - Checksums - Data correcting codes - Availability

Tools for Availability
- Physical protections
- Computational Redundancies.

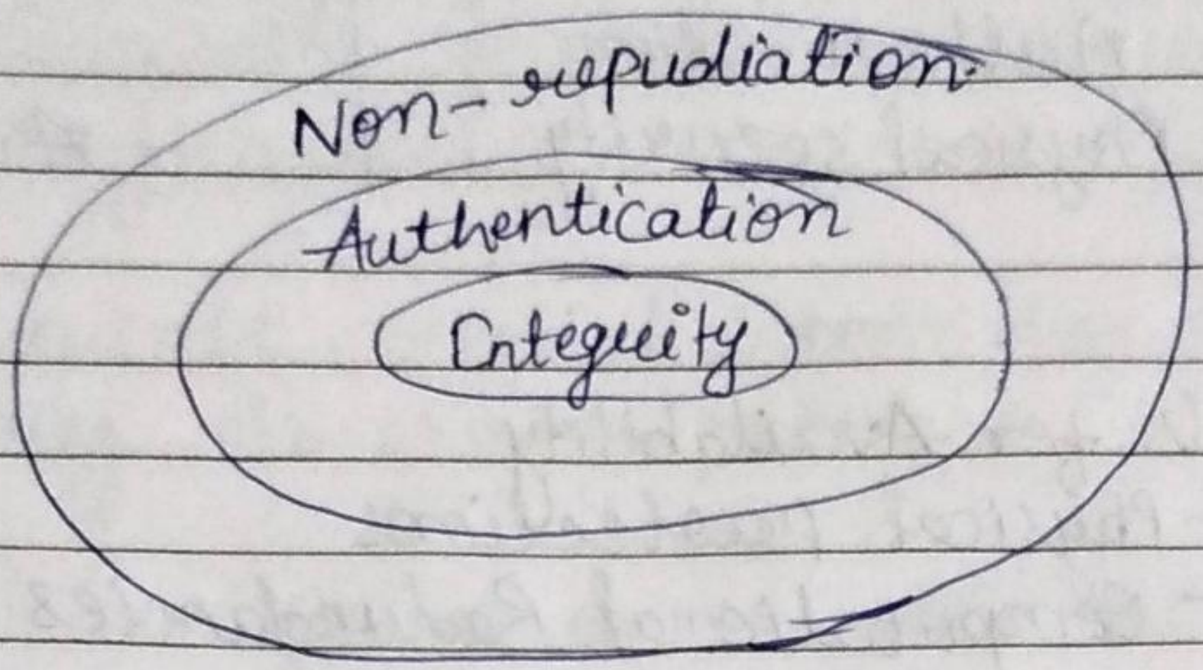
** CIA or CIAAAN :-

(other security compo. added to CIA).
- Authenticadion
- Authorization
- Non-repudiation/Accountability.

Authenticity: Verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

Accountability: Being able to trace the responsible party/process/entity in case of a security incident or action.

→ Relationships among integrity, data-origin authentication and non-repudiation.



→ Vulnerabilities, Threats and Controls:

Vulnerability :- a weakness in a security system.

Threat :- circumstances that have a potential to cause harm.

Controls :- means and ways to block a threat, which tries to exploit one or more vulnerabilities.

e.g. New Orleans disaster (Hurricane katrine)

Q. What were city vulnerabilities, threats, and controls?

Vulnerabilities : location below water level, geographical location in hurricane area.

Threats : hurricane, dam, damage, terrorist ~~attack~~ attack.

Date : / /
Page :

controls :— dams and other civil infrastructures, emergency response plan.

Attacks

A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.

Cyber-attacks can be classified into the following categories:
- Web-based attacks
- System-based attacks.

→ **Security Threats :—**

Threat Spectrum

- Local threats
  - Recreational hackers
  - Institutional hackers
- Shared threats
  - Organized crime
  - Industrial espionage
  - Terrorism
- National security threats
  - National intelligence
  - Info warriors.

Kinds of Threats

- Interception/ Disclosure:
  - an unauthorized party (human or not) gains access to an asset.
  - Snooping: the unauthorized interception of information.

- Interruption/ Disruption:
  - an asset becomes lost, unavailable or unusable.
  - prevention of correct operation.
  - Denial of Service (DOS) attack.

- Modification:-
  - an unauthorized party changes the state of an asset.
  - Masquerading or spoofing.

- Fabrication:
  - an unauthorized party counterfeits an asset
  - inserts fake objects into the system.

→ The S.T.R.I.D.E model of threats:

S	Spoofing → Authenticity
T	Tampering → Integrity
R	Repudiation → Non-repudiation
I	Info. disclosure → Confidentiality
D	Denial of service → Availability
E	Elevation of Privelge → Authorization

→ Spoofing :- The attacker steals your identity.

→ Tampering : The attacker alters your data.

→ Repudiation: The attacker makes your system believe a transaction never happend.

→ Information disclosure: The attacker publishes confidential information.

→ Denial of service: The attacker makes a system unavailable.

→ Elevation of privilege: The attacker gets administrator rights on the system.

** Cyberspace :- A global domain within the information ~~ee~~ environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers.

→ Challenges :-

(i) Innumerable entry points to internet.
(ii) easy to misdirect attribution to other parties.
(iii) Protection from critical operations
(iv) Attack technology outpacing defense technology
(v) Nation states, non-state actors, and individuals are at a peer level, all capable of waging

attacks.

** Critical Security challenges:

- Infiltrations and ransomware
- Policy evasion
- Malicious file transfer
- Command and control
- Data exfiltration.

** EMOTET

- First discovered as a banking Trojan in 2014.
- has been one of the most professional and long-lasting cybercrime services, ever to exist.

- data theft and extortion through ransomware

- EMOTET employed a fully automated process to deliver infected email attachments to victims' computers.

- hundreds of servers located across the world was used by EMOTET to conduct its operations.

→ 3 aspects of information security :
services, Mechanisms, Attacks.

- Security attacks (and threats)
  - actions that (may) compromise security
- Security services
  - services counter to attacks
- security mechanisms
  - used by services
  - e.g. Secrecy is a service, encryption is a mechanism.

Attack

- An attack occurs when someone attempts to exploit a vulnerability.
- Type of attacks
  - Passive (e.g., eavesdropping)
  - Active (e.g., password guessing, Dos)
- A compromise occurs when an attack is successful.

→ Key information Security Concepts :-
- Computer can be subject or object of an attack:
  - When the subject of an attack
    - An active tool to conduct attack

- When the object of an attack
  - An entity being attacked

* Information security vs. access -
  - Perfect security is impossible.
  - Security is a process.
  - security should be considered balance b/w protection and availability.
  - Must allow reasonable access, yet protect against threats.

→ Attacks on computer systems:
  - break-in to destroy information.
  - break-in to steal information
  - blocking to operate properly.
  - Malicious s/w
    - wide spectrum of problems.

- Source of attacks:
  - insiders
  - outsiders

→ Attacker Motives :-

→ Access	→ Influence
- Network	- Hactivism
- Application	- Blackmail
- Data	- Extortion
	- Reputation Damage

Date : __/__/__
Page : _____

Profit

- Financial Transactions
- Identity Theft
- Ransom
- Sell for Profit
- Trade for Services.

* Attack Types :-

(i) Tools or S/W
- Exploit kits
- Tool kits
- keyloggers
- Banking Trojans
- Phishing

(ii) Technical
- Vulnerabilities
- Exploits
- Brute Force
- DNS Hijacking
- Vulnerabilities
- Input Capture
- Sniffing

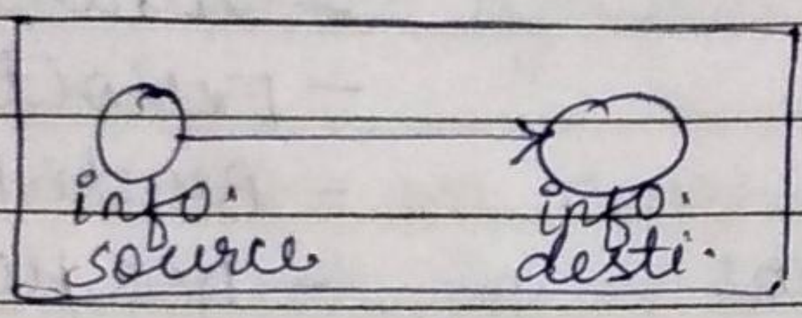
(iii) Non-Technical
- Phising
- Social Engineering
- Stolen Credentials
- Social Engineering
- Dumped Databases
- Leaked Credentials.

* Defense Considerations:

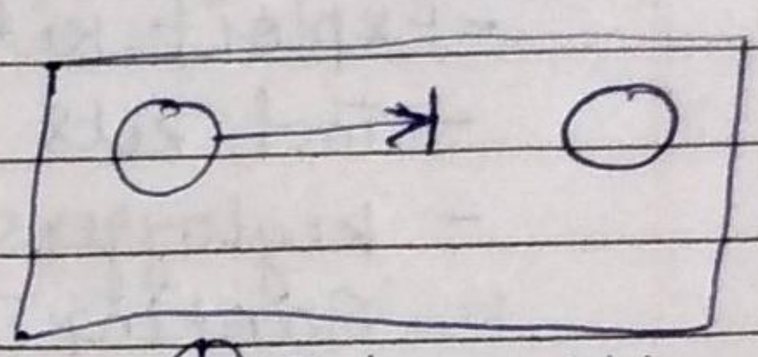
1) Implement multifactor authentication
2) Segment your network environment
3) Enforce "least privilege" and segregation of duties
4) Implement network activity and data leak monitoring

5) Prioritize patching
6) Segment your network environment
7) Enforce secure coding
8) Implement application gateway firewalls
9) Perform regular vulnerability scanning
10) Train employees to be vigilant against phising attacks.

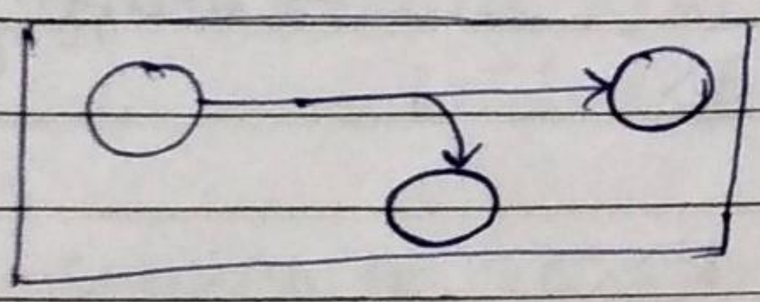
→ Security Threats / Attacks



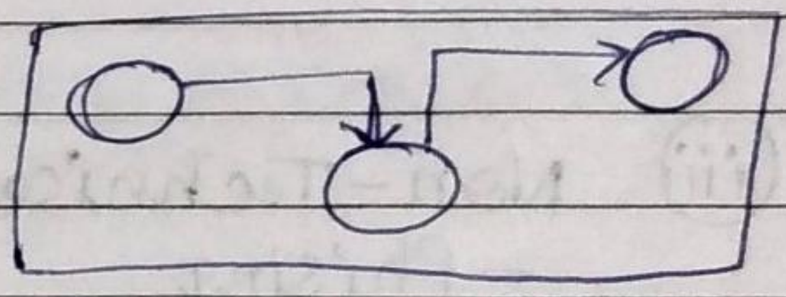
(a) Normal flow



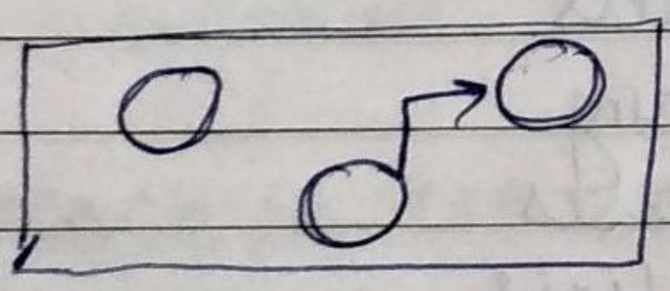
(b) Interruption



(c) Interception



(d) Modification



(e) Fabrication

Active attacks

In active attacks, the attacker intercepts the connection and efforts to modify the message's content. It is dangerous for

integrity and availability of the message.
Active attacks involve Masquerade, Modification of message, Repudiation, Replay, and Denial of service.
- The system resources can be changed due to active attacks.

- So, the damage done with active attacks can be harmful to the system and its resources.

- Active attacks can be prevented by using some techniques.

- We can try the below-listed measures to prevent these attacks -
  - Use of one-time password help in the authentication of the transactions b/w two parties.

Passive attacks :-

In passive attacks, the attacker observes the messages, then copy and save them and can use it for malicious purposes.
The attacker does not try to change the information or content he/she gathered.

Unlike active attacks, in passive attacks, victims do not get informed about the attack.

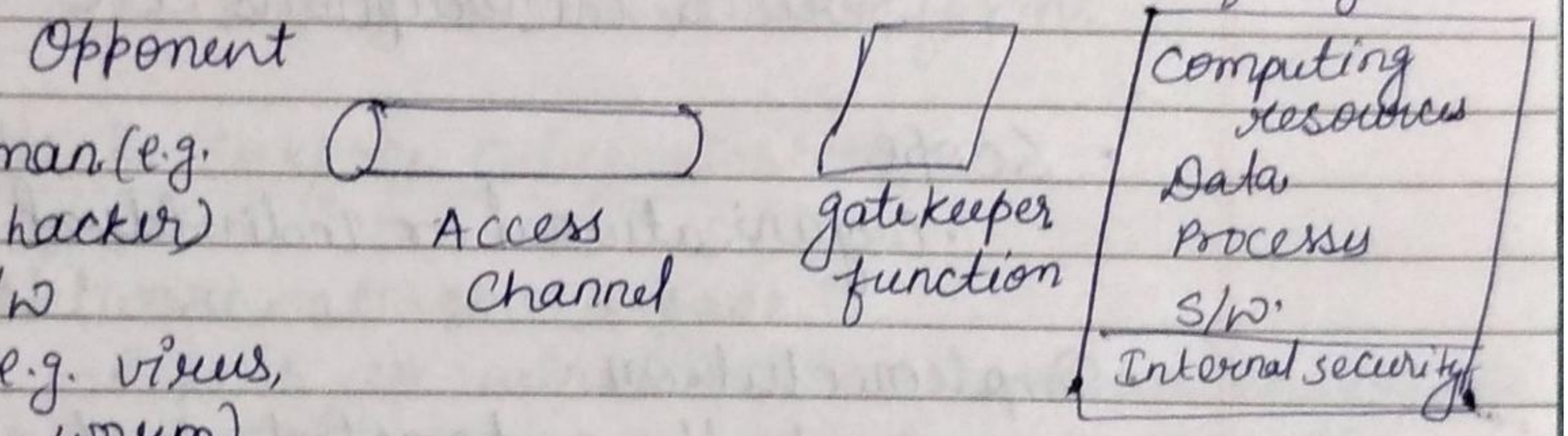
— Passive attacks can be prevented by using some encryption techniques.

Diff^n b/w Active attack and Passive attack :-

** Security services :-

- to prevent or detect attacks
- to enhance the security
- replicate functions of physical documents
  e.g.
  - have signatures, data
  - need protection from disclosure,
  - tempering or destruction
  - notarize
  - record.

→ Model for network Access security :-



- Using this model requires us to:
  - Select appropriate gatekeeper functions to identify users and processes and ensures only authorized users and processes access designated info. or resources.
  - Internal control to monitor the activity and analyze info. to detect unwanted intruders.

→ Move on Computer System Security :-

- Based on "Security Policies"
  - Set of rules that specify
    - How resources are managed to satisfy the security requirements.
    - Which actions are permitted which are not.
  - Ultimate aim
    - Prevent security violations such as unauthorized access, data loss, service interruptions, etc.
  - Scope
    - Organizational or Individual
  - Implementation
    - partially automated, but mostly humans are involved.
  - Assurance and Evaluation
    - Assurance : degree of confidence to a system
    - security products and systems must be evaluated using certain criteria in order to decide whether they assure security or not.

Date : __/__/__
Page : _____

Attack Surfaces

- An attack surface consists of the reachable and exploitable vulnerabilities in a system.
- Examples :
  - Open ports on outward facing Web and other servers, and code listening on those ports.
  - Services available in a firewall
  - Code that processes incoming data, email, XML, office documents etc.
  - Interfaces and Web forms

→ **Attack surface Categories :-**

(i) Network attack surface :
- Refers to vulnerabilities over an enterprise network, wide-area network, or the Internet
  - e.g. DoS, intruders exploiting network protocol vulnerabilities

(ii) Software attack surface
- Refers to vulnerabilities in application, utility, or operating system code.

(iii) Human attack surface :
- Refers to vulnerabilities created by personnel or outsiders
  - E.g. social engineering, insider traitors.

* Anatomy of Attack :-

1	2	3	4	5	6	7	8
Motive	Discover	Probe	Penetrate	Escalate	Expand	Persist	Execute
Objective/ Resources	Data Gathering/ Target identification	Identify Vulne./ Scanning/ Enumeration	Gain Access/ Create Foothold	Crane Escalated Privileged/ Root ACCESS	Multiple Footholds/ Backdoors	obfuscate Presence	Exploit/ Exfiltration/ attack to achieve obj.

→ Fundamental Dilemma of security :-

"Security unaware users have specific security requirements but no security expertise."

Sol?: level of security is given in pre-defined classes specified in some common criteria.

→ Fundamental Trade Off

- Between security and ease-of-use
- Security may require clumsy and inconvenient restrictions on users and processes.

"If security is an add-on that people

have to do something special to get, then most of the time they will not get it".

* Good Enough Security :-
"Everything should be as secure as necessary but not securer".

→ Information Security and Cryptography Technologies :-

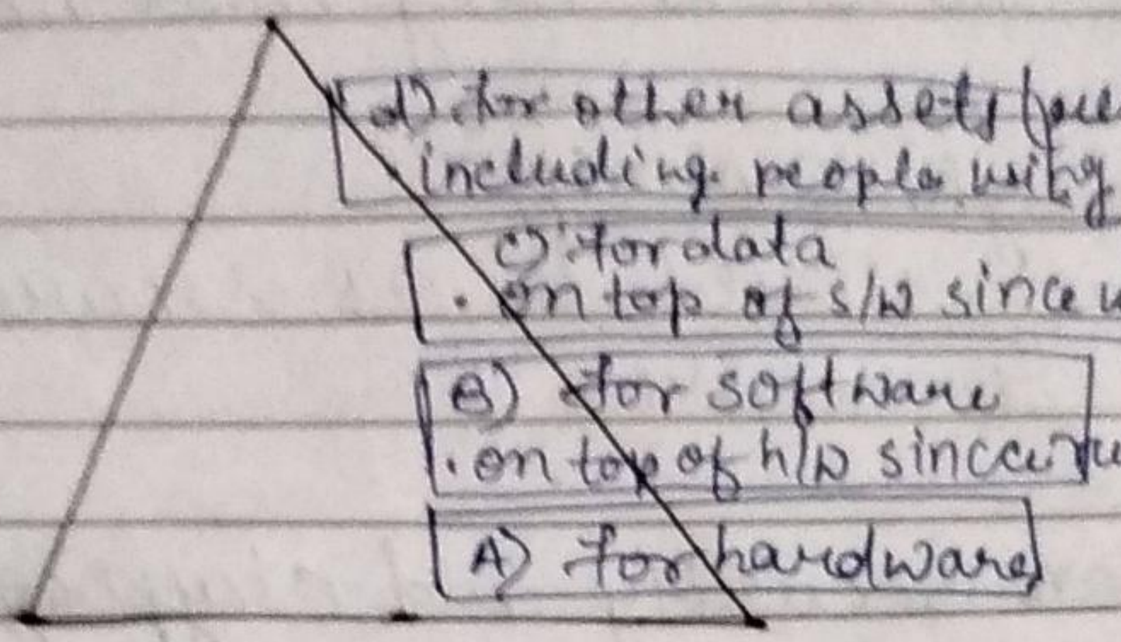
1. System Security Technology :-
   - Protecting Peripheral Components
   - Protecting Distributed Contents
   - Trusted Computing Platforms
   - Detecting Intrusion/ Malware
   - Protecting Data/Access Control
   - Authentication

2. Network Security Technology
   - Protecting Privacy or Anonymity
   - IEEE 802.11
   - Security Pairing

3. Wireless Network Security Technology:
   - security at particular protocol layers
   - Detecting Malicious traffic
   - key Management

4. Cryptography :-
   - Symmetric Cypher
   - Asymmetric Cypher
   - Secure Hashing

Levels of Vulnerabilities / Threats :



	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted CDROM or DVD is stolen.	
Software	Programs are deleted, denying access to users.	An unauthorized copy of s/w is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.

Communication Lines and Networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

(A) Hardware Level of Vulnerabilities/Threats :-

- Add/remove a h/w device
  - Ex :- Snooping, wiretapping

    Snoop :- to look around a place secretly in order to discover things about it or the people connected with it.

    e.g. Modification, alteration of a system.
- Physical attacks on h/w ⇒ need physical security : locks and guards
  - Accidental (dropped PC box) or voluntary (bombing a computer room).
- Theft/destruction
  - Damage the machine (Spilled coffee)
  - Steal the machine.

→ Physical Security has three important components:-
  (i) Access control
  (ii) surveillance
  (iii) testing

→ Example of Snooping:
  Wardriving / Warwalking, Warchalking.

Wardriving / Warwalking: driving / walking around with a wireless-enabled notebook looking for unsecured wireless LANs.

Warchalking: using chalk markings to show the presence and vulnerabilities of wireless networks nearby.
e.g. a circled "W" - indicates a WLAN protected by Wired Equivalent Privacy encryption.

(B) S/W level of Vulnerabilities / threats:-

(i) S/W Deletion:-
  - Easy to delete needed S/W by mistake.
  - To prevent this: Use configuration management S/W.

(ii) S/W Modification:-
  - Trojan Horses, Viruses, Logic Bombs, Trapdoors, information leaks.

(iii) S/W Theft:-
  - Unauthorized copying
  - Via P2P etc

Types of Malicious code :-

- Bacterium: A specialized form of virus which does not attach to a specific file. Usage obscure.

- Logic bomb - Malicious logic that activates when specified conditions are met. Usually intended to cause denial of service or otherwise damage system resources.

- Trapdoor :- A hidden computer flaw known to an intruder, or a hidden computer mechanism installed by an intruder, who can activate the trap door to gain access to the computer without being blocked by security services or mechanisms.

Trojan horse :- A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

Virus : A hidden, self-replicating section of computer S/W, usually malicious logic, that propagates by infecting another program.

Worm: A computer program that can run independently, can propagate a complete working version of itself onto other hosts on

a network, and may consume computer resources destructively.

(C) Data Level of Vulnerabilities/Threats :-

- Adequate Protection
  - Cryptography
    - Good if intractable for a long time.

- Threat of identity theft.

(D) Vulnerab./Threats at Other Exposure points :-

- Network vulnerabilities/threats.
  - Networks multiply vulnerabilities and threats, due to:

    - their complexity ⇒ easier to make design/implem./usage mistakes.

    - "bringing close" physically distant attackers.

- Access vulnerabilities/threats:
  - Stealing cycles, bandwidth
  - Malicious physical access
  - Denial of access to legitimate users.

- People vulnerabilities / threads :
  - Crucial weak points in security
  - Honest insiders subjected to skillful social engineering
  - Disgruntled employes.

(5) Attackers need MOM:

Method: Skill, knowledge, tools etc. with which to pull off an attack.

Opportunity: Time and access to accomplish an attack

Motive: Reason to perform an attack.

→ Type of Attackers :- classification 1

- Amateurs
  - Opportunistic attackers (Use a password they found)
  - Script kiddies

- Hackers - nonmalicious
  - In broad use beyond security community; also malicious.

- Crackers - malicious
- Career Criminals
- State - Supported spies and info. warriors.

Classification 2

- Recreational hackers / Institutional hackers
- Organized criminals / Industrial spies / Terrorists
- National intelligence gatherers / info warriors

Example: Hacking As Social Protest
- Hactivism
- Electro-Hippies
- DDOS attacks on government agencies
- SPAM attacks as "retaliation".

★ Controls against Attacks :-

Methods of Defense

Five basic approaches to defense of computing systems :

(i) Prevent attack
- Block attack / Close vulnerability

(ii) Deter attack
- Make attack harder

(iii) Deflect attack
- Make another target more attractive than this target

(iv) Detect attack
- During or after

* AES (Advanced Encryption Standard)

→ Symmetric key block cipher
(i.e. same key used for encryption + decryption).

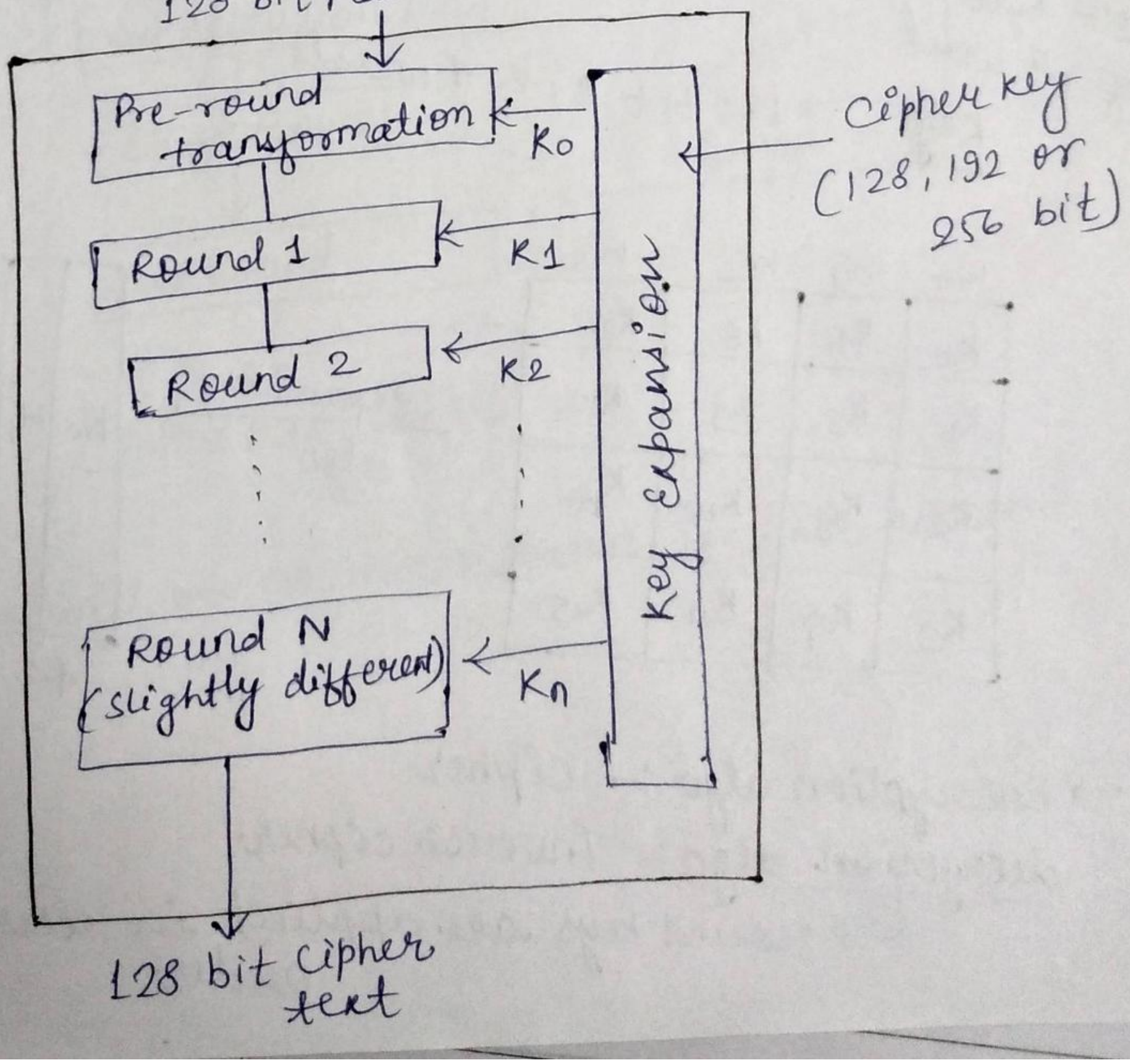
→ established by in 2001 by the U.S. NSIT (National Institute of Standards & Technology).

→ Fixed block size = 128 bits i.e. 16 bytes = 4 words.
(∵ 1 word = 32 bits)

Rounds	no. of bits in key	
10	128	AES-128 version
12	192	AES-192 version
14	256	AES-256 "

→ no. of keys generated by key expansion algorithm = (no. of rounds + 1)

→ General design of AES Encryption:

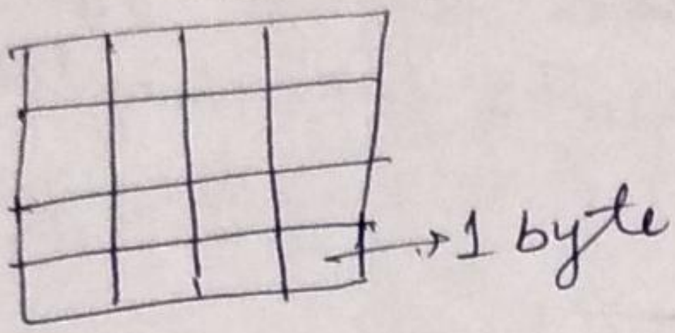


State

16 bytes (4×4)

Stores intermediate result.

Input array (4×4 i.e. 16 bytes i.e. 128 bits) or 4 words.



State array (4×4) 16 byte / 4 word (stores the intermediate result)

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

→ $[W_0, W_1, W_2, W_3]$

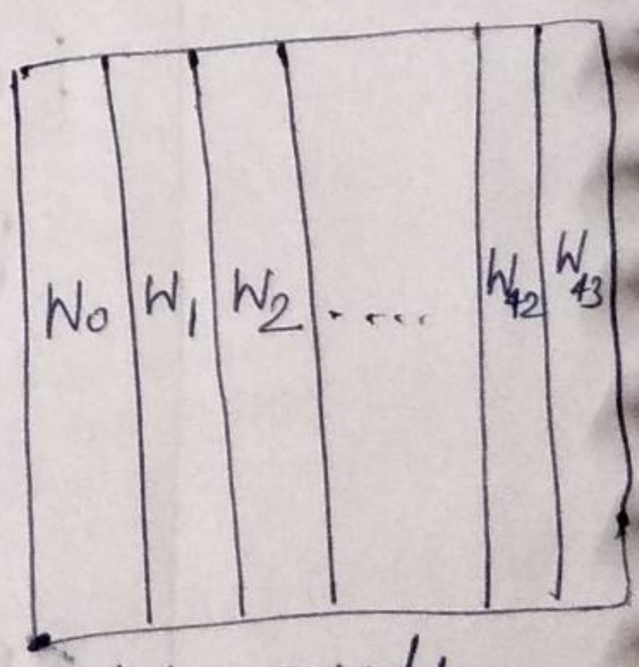
1st byte of 0th word.

2nd byte of 0th word

Key → 128 bit i.e. 4 words.

W_0	W_1	W_2	W_3
K_0	K_4	K_8	K_{12}
K_1	K_5	K_9	K_{13}
K_2	K_6	K_{10}	K_{14}
K_3	K_7	K_{11}	K_{15}

expand key algo →

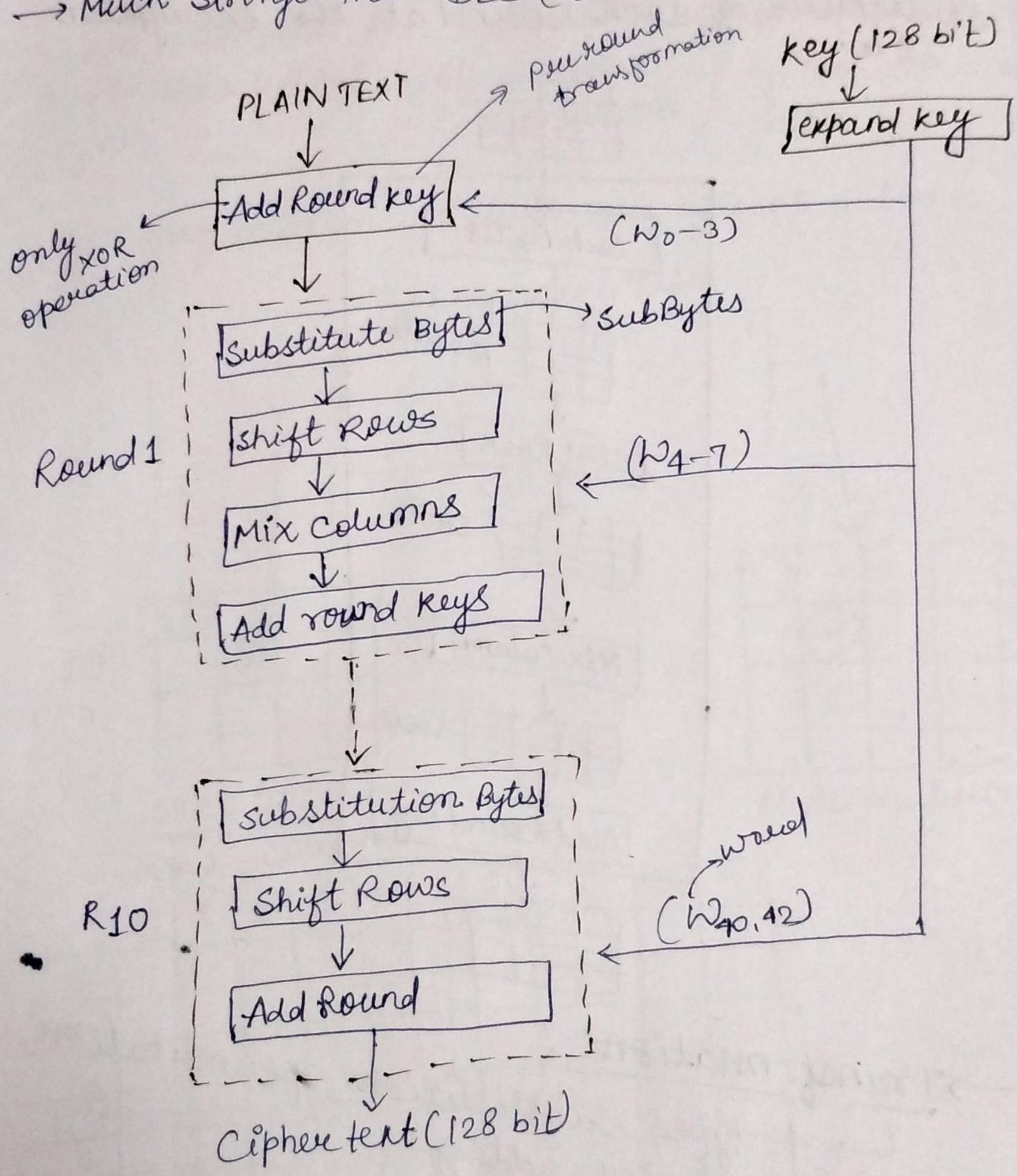


→ Encryption algo :- cipher

decryption algo :- inverse cipher.

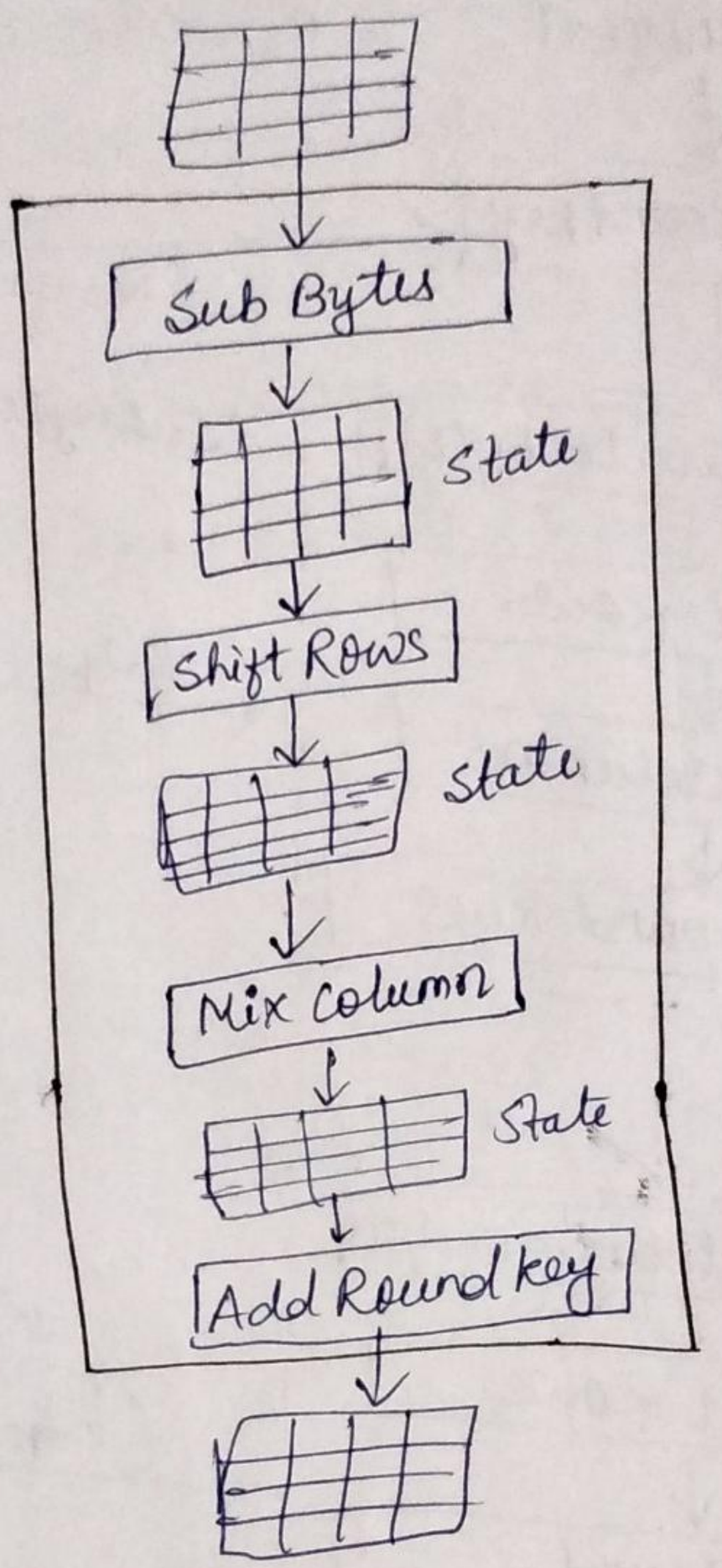
↳ round keys are applied in reverse order.

→ Much stronger than DES (all i.e. 2DES, 3DES)



→ There will be no mix column in last round

Structure of each round at the encryption side.



→ Transformations:
  ↳ 4 types substitution, permutation, mixing and key-adding.

(1) Substitution

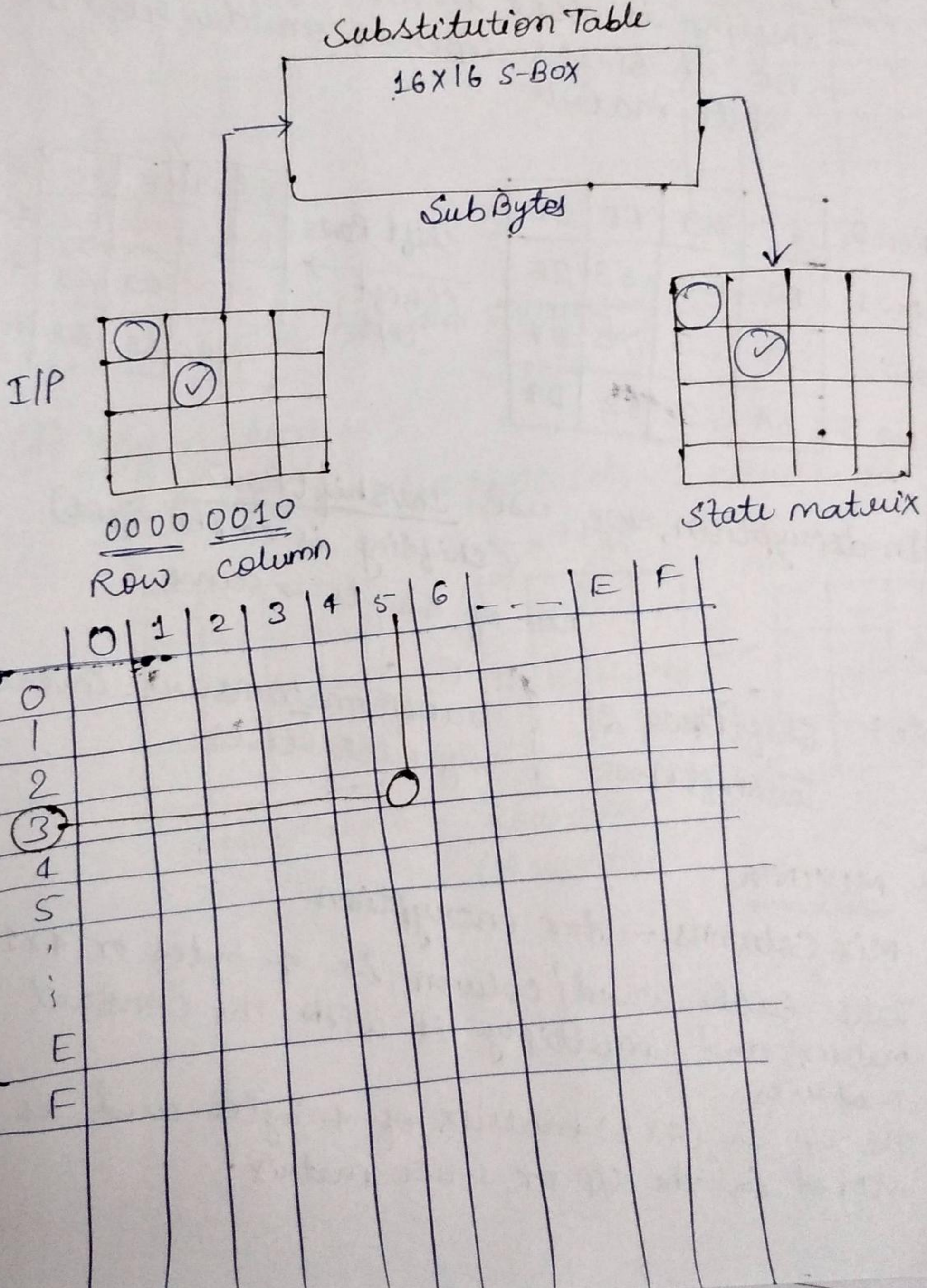
AES, like DES uses substitution but mechanism is dif. Substitution is done for each byte
— only one table is used for transformation of bytes, which means that if 2 bytes are same, the transformation is also same.

SubBytes - at encryption side

We interpret the byte as 2 hexadecimal digits

1st hexadecimal digit → row
2nd " " → column } of the substitution table.

— Transformation is done one byte at a time.



2. Permutation → In this we permute / shift the bytes.

In DES, permutation was done at bit level
In AES, " is " " byte level

→ Shift Rows

- Shifting is done to the left
- no. of shifts depends on the row of the state matrix

Row 0	63	C9	FE	30
Row 1	F2	F2	63	26
Row 2	C9	C3	7D	D4
Row 3	BA	63	82	D4

Shift Rows (Shift left) →

63	C9	FE	30	0 or no shift
F2	63	26	F2	1-byte shift
7D	D4	C9	C3	2-byte shift
D4	BA	63	82	3-byte shift

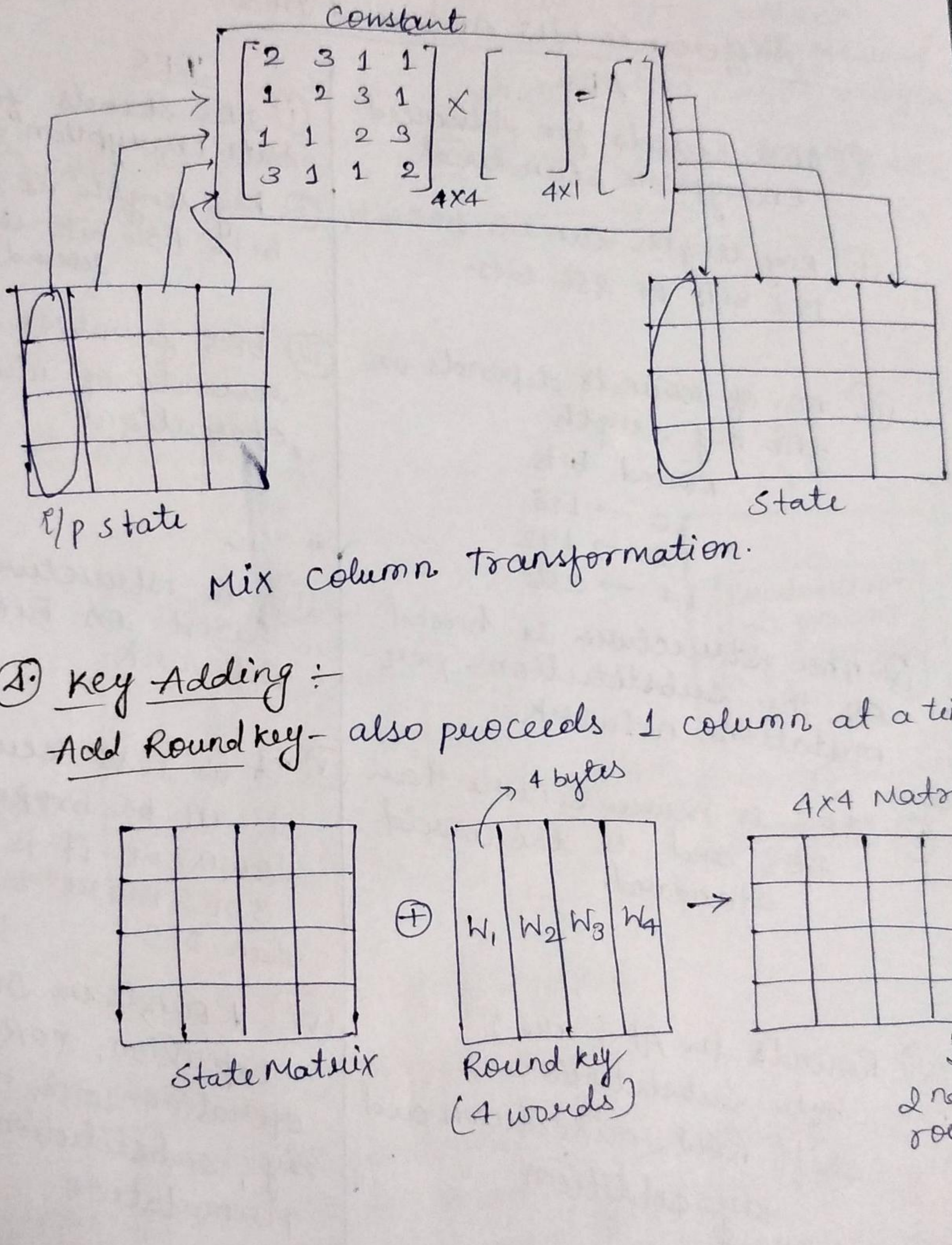
→ In decryption, we use InvShiftRows (shifting is to the right)
no. of shifts → same

Note: ShiftRows & InvShiftRows } transformations are inverses of each other.

3. MIXING

Mix Columns — for encryption.

Take each word/column i.e. 4 bytes or 4x1 matrix and multiply it with the constant matrix.
The o/p is (4x1) matrix of 4 bytes and is stored in the o/p or state matrix.



Mix column transformation.

④ Key Adding :-

Add Round key - also proceeds 1 column at a time.

→ Difference b/w AES and DES

AES	DES
(i) AES stands for Advanced Encryption standard.	(i) DES stands for Data Encryption standard.
(ii) Key length can be 128 bits, 192 bits or 256 bits.	(ii) Key length is 64 bits (56 bits in each round).
(iii) no. of rounds depends on the key length. Round bits 10 → 128 12 → 192 14 → 256	(iii) DES involves 16 rounds of identical operations.
(iv) The structure is based on the substitution-permutation network.	(iv) The structure is based on Fiestel network.
(v) AES is more secure than DES and is the world standard.	(v) It is less secure. It can be broken down (i.e. it is weak). 3DES more secure than DES.
(vi) Rounds in AES are: byte substitution, Shift Row, mixcolumn and key addition.	(vi) Rounds in DES are: Expansion, XOR operation with round key, substitution and permutation.
(vii) It can encrypt 128 bits of plaintext (i.e. block size is 128 bits).	(vii) It can encrypt 64 bits of plain text.
(viii) It is derived from square cipher.	(viii) It is derived from Lucifer cipher.

(ix) No known attack.	(ix) Brute force attack, linear crypt-analysis and differential crypt-analysis
(x) AES is faster.	(x) It is comparatively slower.

Rivest Cipher 4 (RC4) :-

Stream Cipher

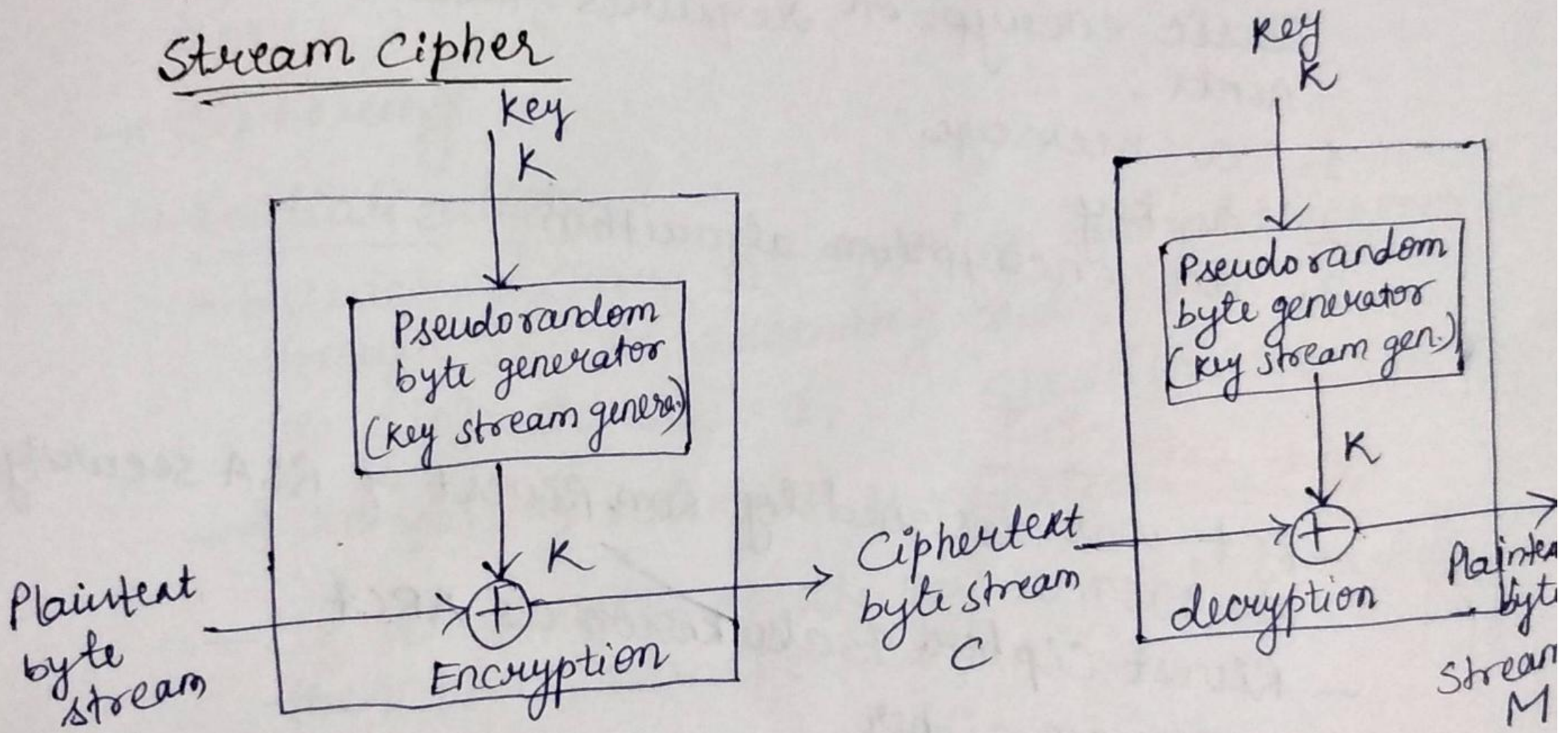


Fig: stream cipher Diagram

→ Exclusive-OR (XOR) operation :-

11001100	plain text	10100000 ciphertext
⊕ 01101100	key stream	⊕ 01101100 key stream
10100000	ciphertext	11001100 plain text

→ How does a stream cipher work?

A stream cipher is an encryption algorithm that uses a symmetric key to encrypt and decrypt a given amount of data.

What makes stream ciphers particularly unique is that they encrypt data one bit, or byte, at a time. This makes for a fast and relatively simple encryption process.

Basic encryption requires three main components:

1. a message
2. a key
3. an encryption algorithm.

RC4 Overview

- RC4 was designed by Ron Rivest of RSA security in 1987.
- Rivest Cipher 4 also known as ARC4.
- a stream cipher
- variable length key algorithm
- encrypts one byte at a time (or larger units on a time)
- simplicity and speed in S/W.

→ The algorithm uses a variable length key from 1 to 256 bytes to initialize a 256-byte state table.

→ The state table is used for subsequent generation of pseudo-random bytes and then to generate a pseudo-random stream which is XORed

with the plaintext to give the ciphertext.

→ Each element in the state table is swapped at least once.

2 phases

- key setup
  - During a N-bit key setup (N being your key length), the encryption key is used to generate an encrypting variable using two arrays, state and key, and N-number of mixing operations.
- ciphering

→ Initialization

- Entries of S are set equal to the values from 0 through 255 in ascending order
  i.e. S[0] = 0, S[1] = 1, --- S[255] = 255.
- A temporary vector T is created.
- If the length of the key K is 256 bytes, then K is transferred to T.

→ Otherwise, for a key of length keylen bytes, the first keylen elements of T are copied from K and then K is repeated as many times as necessary to fill out T.

→ for i = 0 to 255 do
  → S[i] = i ;
  → T[i] = K[i mod keylen];

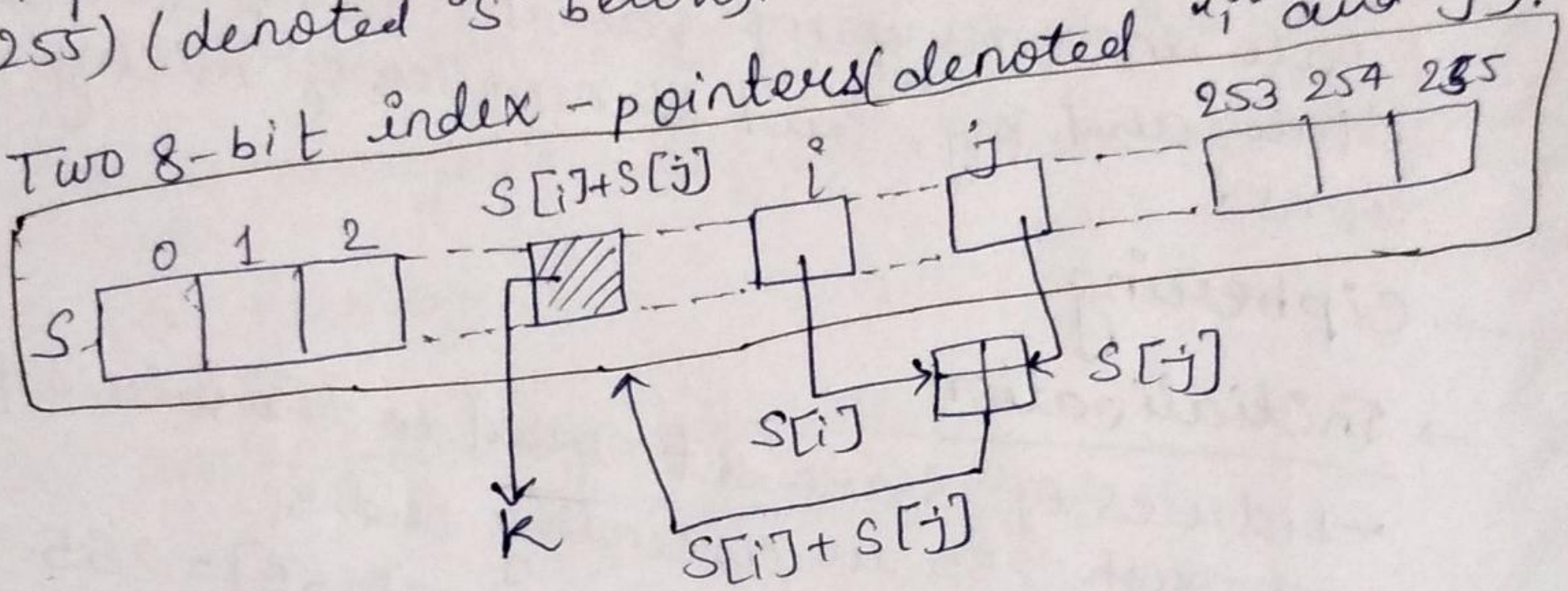
→ Use T to produce the initial permutation of S.

→ Initial Permutation of S :-

- j = 0
- for i = 0 to 255 do
  j = (j + S[i] + T[i]) mod 256;
  swap (S[i], S[j]);

→ Key-scheduling algorithm (KSA)

- A permutation of all 256 possible bytes (0 to 255) (denoted "S" below).
- Two 8-bit index-pointers (denoted "i" and "j").



→ stream Generation:

- i, j = 0;
- while (true)
  - i = (i+1) mod 256;
    j = (j + S[i]) mod 256;
    swap (S[i], S[j]);
    t = (S[i] + S[j]) mod 256;
    K = S[t];

ciphertext[l] = plaintext[l] ⊕ K[l].

Keys

- often limited to 40 bits, because of export restrictions.
- sometimes used as a 128 bit key
- Has the ~~capati~~ capability of using keys b/w 1 and 2048 bits.

→ Strengths of RC4 :-

(i) The difficulty of knowing where any value is in the table.

(ii) The difficulty of knowing which location in the table is used to select each value in the sequence.

(iii) Encryption is about 10 times faster than DES.

RC4 : multiple Vulnerabilities :-

(i) RC4 is no longer considered secure.

(ii) Especially vulnerable when the beginning of the output keystream is not discarded.

(iii) One in every 256 keys can be a weak key. These keys are identified by cryptanalysis that is able to find circumstances under which one of more generated bytes are strongly correlated with a few bytes of the key.

(iv) Vulnerable when nonrandom or related keys are used.

RC4 Example :-

Q. key array = [1 2 3 6], Plain text = [1 2 2 2]

— Initialize the state vector S and temporary vector T.

S = [0 1 2 3 4 5 6 7]

T = [1 2 3 6 1 2 3 6]

— Now perform the initial permutation on S.

(1) -

(1) $j = 0$

for $i = 0$ to 7

$j = [0 + 0 + 1] \bmod 8$

$= 1 \bmod 8 = 1 \Rightarrow j = 1$

swap(S[0], S[1])

So, S = [1 0 2 3 4 5 6 7]

Similarly iterate till $i = 7$.

(2) $i = 1,\ j = 1$

$j = (j + S[i] + T[i]) \bmod 8$

$= (1 + 0 + 2) \bmod 8 = 3 \bmod 8 = 3$

swap (S[1], S[3])

So, S = [1 3 2 0 4 5 6 7]

(3) $i = 2$,

$j = (3 + 2 + 3) \bmod 8 = 8 \bmod 8 = 0.$

swap(S[2], S[0])

So, S = [2 3 1 0 4 5 6 7]; $\Rightarrow j = 0$

$j = (j + S[i] + T[i]) \bmod 8$

(4) $i = 3$,

$j = (0 + 0 + 6) \bmod 8 = 6.$

swap(S[i], S[j])

swap(S[0], S[6])

~~S = [6 3 1 0 4 5 2 7]~~ S = [2 3 1 6 4 5 0 7]

(5) $i = 4$,

$j = (6 + 4 + 1) \bmod 8 = 3$ $\quad j = 3$

swap(S[4], S[3])

S = [2 3 1 4 6 5 0 7]

⑥ $i = 5$

$j = (3+5+2) \bmod 8 = 2$

swap(S[5], S[2])

S = [2 3 5 4 6 1 0 7]

⑦ $i = 6$

$J = (2+0+3) \bmod 8 = 5$

swap(S[6], S[5])

S = [2 3 5 4 6 0 1 7]

⑧ $i = 7$

$J = (5+7+6) \bmod 8 = 2$ (J=2)

swap(S[7], S[2])

S = [2 3 7 4 6 0 1 5].

Hence, our initial permutation of S gives:

S = [2 3 7 4 6 0 1 5];

→ Next step, stream generation

No. of iterations = size of key

└ ④ [iteration 0 to 3].

```
i, j = 0
while (true) {
    i = (i+1) mod 8;
    j = (j+S[i]) mod 8;
    swap(S[i], S[j]);
    t = (S[i] + S[j]) mod 8;
    K = S[t];
}
```

Now key is obtained (used for encryption & decryption)

3.

— The first iteration:

① S = [2 3 7 4 6 0 1 5]

i = (0+1) mod 8 = 1

j = (0+S[1]) mod 8 = 3

swap(S[1], S[3])

S = [2 4 7 3 6 0 1 5]

t = (S[1] + S[3]) mod 8 = 7

K = S[7] = 5

So our first 3-bits of ciphertext is obtained by:

K XOR P(1) = 5 XOR 1 = 101 ⊕ 001 = 100
= 4

(2) S = [2 4 7 3 6 0 1 5]

i = 1

i = (1+1) mod 8 = 2

j = (j + S[2]) mod 8 = (3 + 7) mod 8 = 2

swap(S[2], S[2])

~~S = [2 4 5 3 6 0 1 7]~~ S = [2 4 7 3 6 0 1 5]

t = (S[i] + S[j]) mod 8

= (7 + 7) mod 8 = 6

K = S[6] = 1.

K XOR P(2) = 1 XOR 2 = 001 XOR 010
= 011 = 3.

001
010
011

(3) S = [2 4 7 3 6 0 1 5]

i = (2+1) mod 8 = 3

j = (j + S[i]) mod 8

= (2 + S[3]) mod 8 = (2 + 3) mod 8 = 5

swap(S[3], S[5])

S = [2 4 7 0 6 3 1 5]

t = (S[i] + S[j]) mod 8

= (0 + 3) mod 8 = 3

K = S[3] = 0.

K XOR P(3) = 0 XOR 2 = 000 ⊕ 010 = 2

(4) S = [2 4 7 0 6 3 1 5]

$i = (3+1) \bmod 8 = 4$

$j = (j + S[i]) \bmod 8 = (5 + S[4]) \bmod 8$

$= [5+6] \bmod 8 = 3$

Swap(S[4], S[3])

S = [2 4 7 6 0 3 1 5]

$t = (S[i] + S[j]) \bmod 8$

$= (0 + 6) \bmod 8 = 6.$

$K = S[6] = 1.$

K XOR P(4) = 1 XOR 2 = 001 XOR 010 = 011 = 3.

P = [1 2 2 2]

K = [5 1 0 1]

C = [4 3 2 3]. Ans.

RC4 security :-

- Claimed secure against known attacks.
- However, have some analyses, some on the verge of practical.
- first 256 bytes have bias.
- multiple keys / same plaintext attack
- result is very non-linear
- since RC4 is a stream cipher, must never reuse a key.
- have a concern with WEP, but due to key handling rather than RC4 itself

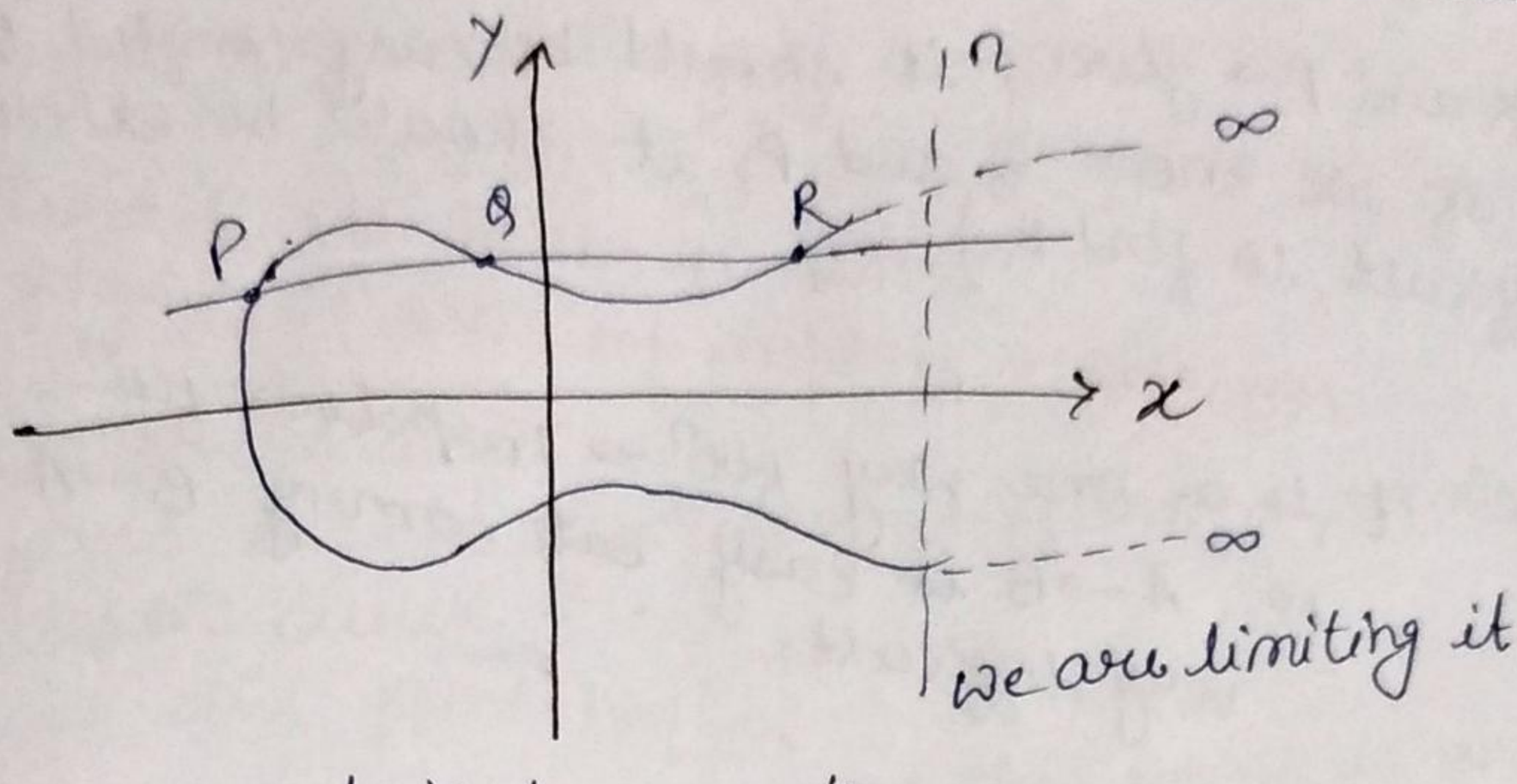
** Elliptic Curve Cryptography :- (ECC)

→ It is asymmetric key encryption.
→ It ~~is~~ provides equal security with smaller key size (e.g. as compared to RSA) as compared to non ECC algos.
⇒ i.e. small key size and high security.
→ It makes use of Elliptic curves.
→ Elliptic curves are defined by some mathematical functions - cubic fun.

e.g. $\boxed{y^2 = x^3 + ax + b}$ // equation of degree 3

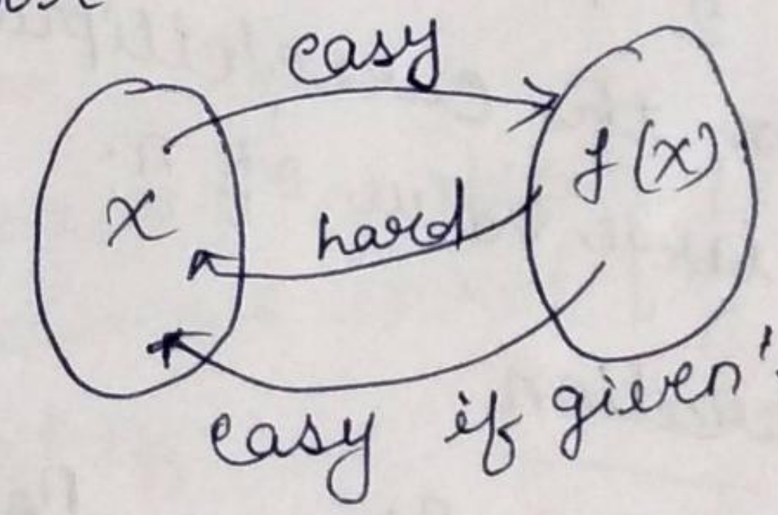
→ The no. of points N is bounded by:

→ $p+1-2\sqrt{p} <= N <= p+1+2\sqrt{p}$.



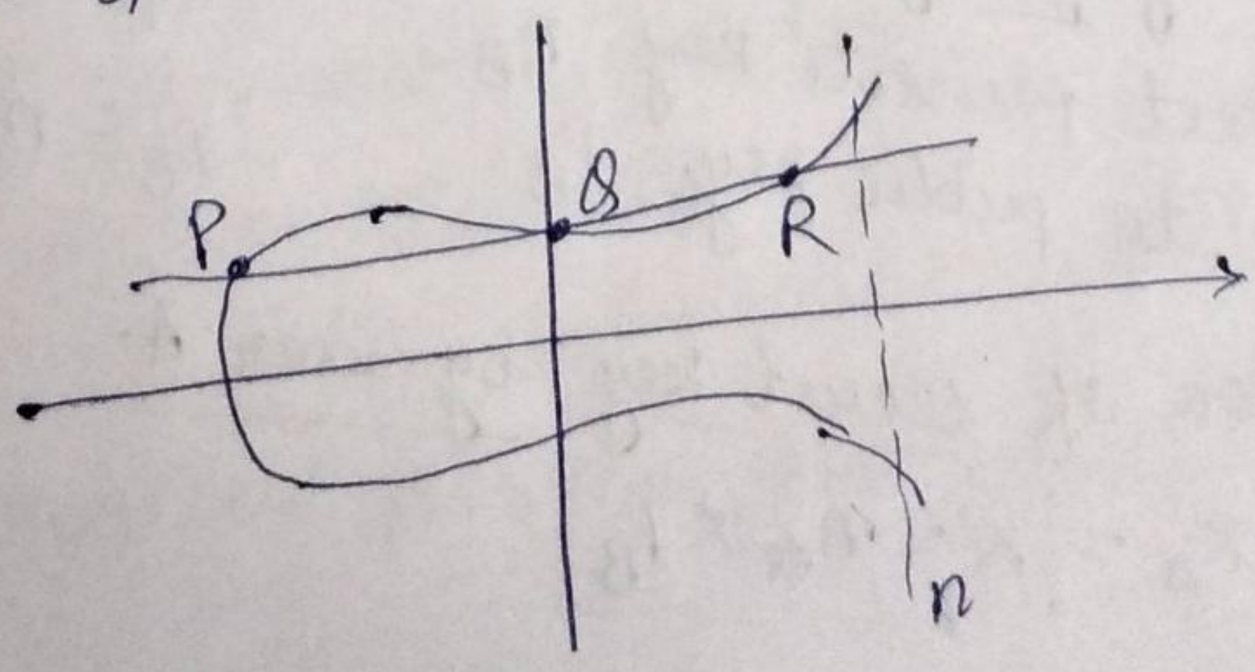
→ Symmetric to x-axis
→ If we draw a line, it will touch a max of 3 point.

A Trapdoor function is a fn that is easy to compute in one dirn, yet difficult to compute in the opposite direction (finding its inverse) without special information, called the trapdoor.



easy if given 'f' → trapdoor value.

Let $E_p(a,b)$ be the elliptic curve
consider the equation $\boxed{Q = kP}$
where Q, P → points on curve and $k < n$.



(If K and P → given, it should be easy to find Q.
but if we know Q and P, it should be extremely difficult to find K.) this is called the discrete logarithm problem for elliptic curves.

i.e. it is a one way fu° → Trapdoor fu°?

ie. A → B is easy but coming B → A is very difficult.

ECC - Algorithm

ECC - key Exchange

Global Public Elements

Ea(a,b) : elliptic curve with parameters a, b and q.

q ↓ Prime no. or an integer of the form 2^m.

G : Point on the curve/elliptic curve whose order is large value of n.

User A key generation

Select private key n_A $\quad n_A < n$

Calculate publickey P_A $\quad \boxed{P_A = n_A * G}$

User B key ~~gen~~ generation

Select private key n_B $\quad n_B < n$

Calculate public key P_B. $\quad \boxed{P_B = n_B * G}$

Calculation of secret key by user A.

$K_A = \boxed{K = n_A * P_B}$

Calculation of secret key by user B

$$K = n_B \times P_A$$

ECC Encryption

- Let the message be M.
- first encode this message M into a point on elliptic curve.
- Let this point be P_m.
  ↳ now this point is encrypted.

for encryption, choose a random positive integer k.

The cipher point will be → for encryption Public key of B used.

$$C_m = \{kG, P_m + kP_B\}$$

This point will be sent to the receiver.

Decryption

for decryption, multiply 1st point in the pair with receiver's secret key.

i.e. $kG * n_B$ // for decryption private key of B used.

Then subtract it from 2nd point / coordinate in the pair

i.e. $P_m + kP_B - (kG * n_B)$

but we know $P_B = n_B * G$

So $= P_m + kP_B - kP_B$

$= P_m$ (original point)

→ so receiver gets the same point.

ECC Vulnerabilities

Side-channel attacks : differential power attacks, fault analysis, simple power attacks, and simple timing attacks. typically result in information leaks. Simple countermeasures exist for all types of side-channel attacks.

Twist-security attack or fault attack:

Such attacks may include invalid-curve attacks and small-subgroup attacks, and they may result in the private key of the victim leaking out.

Twist-security attacks are typically simply mitigated with careful parameter validation and curve choices.

ECC Vs RSA

Security (bits)	DSA/RSA	ECC
80	1024	160-223
112	2048	224-255
128	3072	256-383
192	7680	384-511
256	15360	512+

→ EC Digital Signature Algo. (ECDSA)

- User A generates key pair using ECC.
- Then generates it's signature.
  1. select a random or pseudo-random integer K, $1 \leq K \leq n-1$.
  2. Compute $X = K \cdot G_r \bmod p = (x, y)$ and $r = X \bmod n$
     if $r = 0$ then go to step 1.
  3. Compute $K^{-1} \bmod n$.
  4. Compute $e = SHA1(m)$.
  5. Compute $s = K^{-1}\{e + xr\} \bmod n$ if $s = 0$ then go to step 1.
  6. A's signature for the message m is (r, s).

→ EC Digital Signature Algo. (ECDSA) Verification:

- User A generates key pair using ECC.
- Then generates it's signature.
  1. A's Public key (E, G_r, n, P).
  2. Verify r, and s are integer in K,
     $1 \leq r, s \leq n-1$.
  3. Compute $e = SHA1(m)$.
  4. Compute $w = s^{-1} \bmod n$
  5. Compute $u_1 = ew \bmod n$ and
     $u_2 = rw \bmod n$
  6. Compute $G_r \cdot u_1 + P \cdot u_2 \bmod p = (x_0, y_0)$
     and $v = x_0 \bmod n$
  7. Accept signature if $(v = r)$.